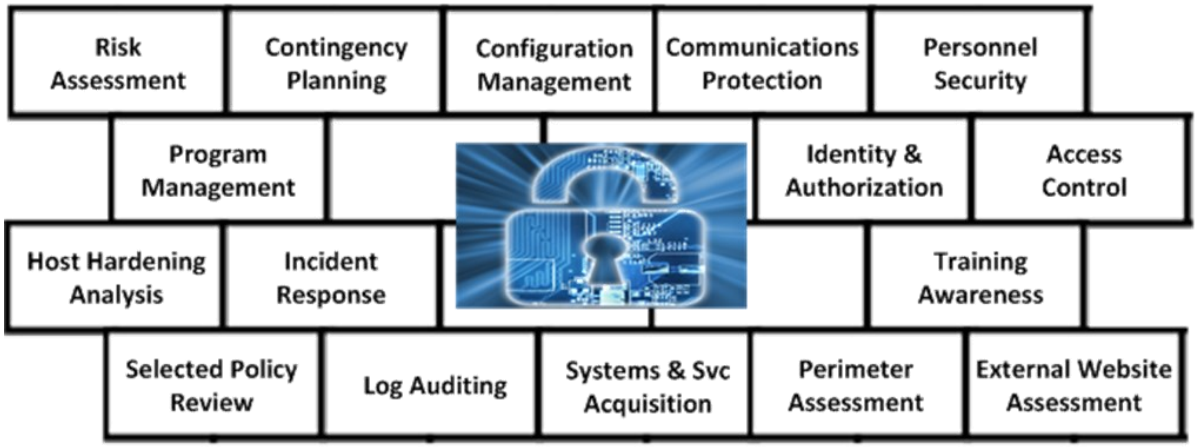
Independent Security Assessment (ISA) Pre-Coordination Preparedness Guide

Pre-Assessment Materials Preparation, On-Site Configuration Requirements, and Personnel Availability Impacts on Assessed Organizations

Version 1.3, Dated 9/1/2016

What is the Independent Security Assessment (ISA)?

The ISA is a mandated assessment as outlined in California State Code 11549.3, as amended on January 1, 2016 and is sometimes referred to as an AB670 assessment. The purpose of the ISA is to assess an identified subset of NIST controls, at the Moderate level, to measure the moment in time cybersecurity processes, practices, and configurations of the enterprise. Due to the number of controls assessed, hosts analyzed, and interviews conducted, this process typically takes multiple days on site, depending on the size of the entity assessed. To ensure your assessment process is smooth and causes the least amount of impact on your staff, a series of pre-assessment preparation steps are provided within this guide. The CND assessment team will arrive at the designated location and time of your assessment. We simply request the entity be prepared and ready for assessment. Due to the constrained timeline for assessment, missing documentation or unavailable staff could adversely impact the entities overall results.



Entities Formally Selected for Assessment

Most entities begin the assessment process when they are formally notified by the Chief Information Officer's (CIO) office. A formal notification letter requires the entity management team to acknowledge the receipt in one of two manners:

1. Open a Service Ticket with CDT to schedule and ISA; assessment service windows are filled on a first come, first serve basis.
2. Deliver a formal waiver request package to the State Chief Information Security Office (CISO) within 10 calendar days of the date of the notification letter. There are finite criteria for exemption and waivers (e.g. proof of a pre-existing executed contract for an ISA provided by a 3rd party along with a cross-walk of the Scope of Work to the ISA Assessment Criteria). For more information please have your CIO contact the State Information Security Office.

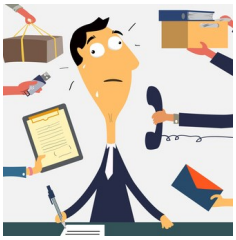
Note: Organizations not approved for exemption could risk severely limited choices of remaining Assessment service windows.

Can My Organization Be Pre-Assessed or Volunteer for an ISA this Year?

Absolutely! We have had a number of organizations elect to undergo both selected portions or full assessments depending on their needs, timelines, and budgetary constraints. These services can be a tremendous tool in helping understand and prioritize future cybersecurity goals as well as remediate potential shortfalls. If you are interested in learning more about the various options available to your organization and how a partial assessment differs from scheduled assessment, please contact the CND at the numbers provided in this guide

What is the Staff Impact to my Organization?

The ISA process is based on the criteria established by California's Chief Information Security Officer. As the criteria moves into new phases the Tasks, Conditions, and Standards of evaluation change. These all impact both the assessed organizations participation requirements and the time for completion. Rest assured, the CND makes every attempt to streamline this process to minimize the time requirements on your team. Typically the team can conduct a large portion of the process with minimal staff interaction. These portions generally consist of captures of network traffic, vulnerability scanning hosts, and system hardening analysis. Portions that will impact your staff's time generally include areas where privileged logon to perimeter devices are required to document or analyze a particular setting, initial in-briefings, coordination for credentials or other system / network administrator focused tasks, and of course the interview process. The CND typically can complete an assessment within 1-3 weeks depending of your organizations size. Individual staff impacts ranged from minutes to several hours depending on their role and readiness for assessment Its our goal to get your team back to work doing their daily operations.



Guide Purpose

This guide is designed to help the assessed organization prepare for successful assessment. It is critical this document be disseminated to the responsible individuals within the entities' Cybersecurity and IT organization whom will be conducting the required pre-assessment configurations and documentation. *The entity senior cybersecurity manager is responsible to ensure the organization is ready for their assessment prior to the start date*. Delays or missing documentation prevent the assessment team from rendering a complete assessment in the time frame allotted and may result in *non-compliance findings* in those incomplete / improperly prepared areas. Please help us help you achieve the most benefit possible from this program by ensuring your readiness for assessment.

Guide Usage

This guide is divided into 4 sections, based on generally accepted functional roles within an Information Technology organization. These sections are:

- Information Security Management
- Network Administrator Actions
- System Administrator Actions
- Human Resources / Training Actions

Information Security Management:

Pre-Assessment Requirements:

- Initiate either the ISA Service Request (Appendix A)
    - If you are submitting Request for Waiver to the CIO's Office, the completed Request must be received within 10 calendar days of the notification letter date.
- Complete the Entity Asset Count Worksheet (Appendix B), append the service request ticket number to the information, and email to the CND Engagement Mgr
- Coordinate with engagement manager to select your assessment window from the dates available
- Complete the Assessment Questionnaire (provided upon scheduling) prior to the Pre-Assessment Status Conference Call; add to the documentation CD ROM to be provided during the Assessment In-briefing (Appendix C)
- Schedule the entities Pre-Assessment Status Conference call no less than 3 weeks prior to your engagement date
- Prepare copies of the required policies (Appendix D), to be delivered to the CND Team Lead during the initial in-brief on Assessment day 1.
- Coordinate a work location for the assessment team. The location must be able to accommodate no less than 2 dedicated Cat5/6 network data jacks capable of >=100Mbps. If possible, the space should support securing equipment over night.
- Coordinate for a conference room capable of conducting the initial Assessment Team in-brief
- Schedule the meeting with the appropriate entity staff members and management team(s) that will be participating in the assessment

- Designate and provide a minimum of 100 users (3 Executive, 3 Admins, and a mixture of all entities' business units) for participation in the Phishing Susceptibility Test. If the organization wishes a larger population set to participate in the exercise, please coordinate with the CND Engagement Manager.

    - Provide CSV file with the following field completed for each nominated user to the CND Engagement Manager no less than the Wednesday of the week prior to the assessment date:

        FirstName, LastName, EmailAddress

    - The entity is prohibited from notifying the designated users they have been nominated
- Designate the public-facing web site for assessment to the CND Engagement Manager no less than 5 calendar days prior to the assessment date. If this site is hosted at a State Data Center or 3rd party host, the entity must pre-coordinate the scan with the service provider; documentation is required at the Pre-Assessment brief.
    - If site requires credentials for access to any public facing portions, generate a Standard user account for the system for testing and provide to the CND Engagement Manager

<u>Assessment Period Requirements</u>:

- Provide the team members access badges to the facility for the period of the assessment
- Act as the facilitator between the CND Team Leader and entity staff
- Coordinate with senior management to ensure all required personnel for the assessment are scheduled to be in attendance at the assessment location for the entire assessment period
- Identify the Primary Points of Contact, locations, and phone numbers for the Network, Systems, Support Desk, and Human Resources designed points of contact during the assessment.
- Report Phishing detection (as applicable) to the on-site CND Team Leader (This is how the entity receives detection credit). Note: The exercise is designed to test the viability of the user education process, not the Incident Response capabilities of the entity
    - The entity is prohibited from:
        - Notifying users once detected
        - Blocking the email domain or associated website

- Reporting the Incident in Cal-CSIRS (wastes valuable IR resources)

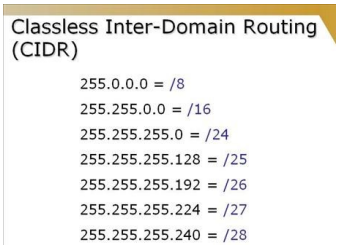
Post Assessment Requirements:

- Coordinate with internal entity management teams for Assessment Out-brief
- Notify any users who surrendered credentials during the Phishing exercise they must reset their passwords (List to be provided by CND upon conclusion)
- Whitelist the Phishing Domain and Website (if initial test is blocked automatically); **CND will notify the entity if this action is required**
- Designate the primary and alternate recipients for the final report delivery
- Prepare and submit the POA&M for CDT based on the developed mitigation strategy

Network Administrator Actions:

Pre-Assessment Requirements:

- Ensure the network drops provided to the assessment team have full WAN / LAN / VLAN access to all entity IT assets (e.g. workstations, laptops, servers across all locations and subnets). Test access to ensure there are no blocking Access Control Lists (ACLs)
- Ensure ports 22,135,137,139, and 445 are allowed to travers all internal network segments during the assessment period
- Provide the CND Team leader with a Networking team representatives work location, phone number, and email to facilitate troubleshooting (if required)
- Prepare the Network Interconnection diagram and provide it to the senior cybersecurity manager
- Prepare 2 static IP address for the CND Team Scanners that are tied to the appropriate VLAN listed above (4 IP's if port-based security restrictions are in place to accommodate the host and VM for each laptop)



- Prepare a text file that contains a list by Class C address space of the location of your IT assets (e.g. Users: 10.0.100.0/24; 10.0.101.0/24; & Servers: 10.0.103.0/24); provide the list to the senior cybersecurity manager for inclusion on the CD-ROM provided to the team leader at the in-brief.
- *Notify the assessment team **within 5 days** of their arrival if the entity if:*
  - *IPv6 addressing is used in the environment for the servers, workstations, or laptops*
  - *If host are scatters across excessively large IP address Spaces (e.g. /16 or /8 CIDR ranges).*

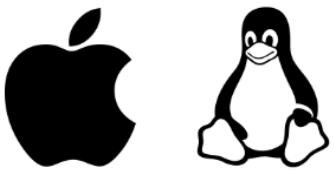
Assessment Requirements:

- Be available for the network portion of the Assessment interview process
- Provide troubleshooting assistance for scan related ACL troubleshooting issues (as needed)
- Deliver the perimeter firewall configuration files (on CD ROM) in accordance with the instructions provided by the CND Team Leader

System Administrator Actions:

Pre-Assessment Actions:

- Domain Systems: Prepare root / domain administrator level credentials for use by the assessment team for all directory joined servers, workstations, and laptops. *If more than one domain is present, prepare this for all domains*. These may be existing credentials provided to the CND Team leader or manually entered by the entity Systems Administrator. Note: If manual entry option is the selected, then the Systems Administrator must co-locate with the team until scanning is completed (typically several days to multiple weeks depending on entity asset count).
- Non-Domain Systems: Prepare root / domain administrator level credentials for use by the assessment team for all non-directory joined servers, workstations, laptops, and appliances. These may be existing credentials provided to the CND Team leader or manually entered by the entity Senior Systems Administrator. The same username/password must work across all such systems. Note: If manual entry option is the selected, then the Senior Systems Administrator must co-locate with the team until scanning is completed (typically several days depending on entity asset count).
- Ensure all Windows operating system hosts "Server" service is running and accept ports 135,137,139, and 445 requests; add exceptions to any host-based firewall and Host-based Intrusion prevent protections for these ports to/form CND static IP addresses or white list the static IP address assigned to these devices (as appropriate) If you have specific concerns, please contact CND immediately.
- Ensure all Linux / Unix / AIX / Macintosh operating systems hosts accept port 22 requests; add exceptions to/from and CND IP addresses to any host-based firewall and Host-based Intrusion prevent protections for this port or white list the static IP address assigned to these devices (as appropriate)



- Whitelist the static IP addresses of the two CND devices with Anti-virus
- Identify 3 workstations and 3 laptops that will be made available for System Hardening scanning. These hosts must not:

- Have user logged on during the assessment period (typically 30 minutes)
- Have any setting that could cause the hosts to sleep or otherwise disconnect form the network; including sleep settings during off hours for the duration of the assessment period.

- Identify 1 Domain Controller and 3 Application servers for System Hardening scanning. This scan will take approximately 30 minutes to complete and will add a minor workload to the host.

Assessment Actions:

- Troubleshoot network credential issues / port issues on hosts (as applicable)
- Provide access to the CND Team Leader to run various PowerShell scripts to validate controls (as required)
- Provide CND Team leader access to AD Users and Computers to perform random sampling selections and validations (as required)
- Be available for the systems portion of the Assessment interview process

Human Resources / Training Manager Actions:

Pre-Assessment Actions:

- Ensure 100% accountability and access to the entities Acceptable Use Policy acknowledgement paperwork; streamline searching for random individual records.
- Ensure 100% accountability of all Network user training records including attendance and content breakdown. If possible, have a hard copy of the content available for the CND Team lead.

Assessment Actions:

- Be available for the Human Resources / Training Manager portion of the Assessment interview process

Clarifications or Assistance

In preparation for your Assessment if you or your team members have questions, please do not hesitate to contact us. To streamline you experience, direct all question to the CND Engagement Manager:

Senior Master Sergeant Alice Allersmeyer

Email: alice.m.allersmeyer.nfg[@]mail.mil Phone: 916-369-5030

Appendix A - Service Request Procedure

In Remedy:

- Open the Remedy Service Ticket Application
- Navigate to the “Professional Services” category
- Select “Independent Security Assessment (ISA)” option

In CSS:

- In the Ticket Title enter “ISA for {Department Name}

Appendix B - Entity Asset Count Worksheet

Asset Category	# of Assets
Number of Windows Servers (Physical and Virtual)	
Number of Linux, Unix, Apple Servers (Physical and Virtual)	
Number of Windows Desktops & Workstations	
Number of Windows Laptops and Convertibles	
Number of Linux / Apple Desktops, Workstations, and Laptops	
Total Asset Count:	

Entity Name: _____ Service Request #:_____

Primary Point of Contact: _____

Email: _____ Phone #:_____

Appendix C - Day 1 DVD-ROM Materials Checklist

Item	Description	Provided
CDT Service Request	For Data Center Hosts assets, provide a screen shot of the ISA Service Request (Include Request #) as applicable	
ISA Questionnaire	Provide an electronic copy of the entities completed ISA questionnaire	
Requested Policies	A completed copy of Annex B listing the mapping between required policies and entity policy name. Please provide in either PDF or XPS format.	
3rd Party Notifications	Provide a copy of any 3rd party hosted / managed IT notifications performed. These are required if an assets is hosted or managed by a 3rd party and CND is scheduled to scan the device. For additional guidance, contact CND.	
Point of Contact Listing	Provide a contact list that includes the First, Last, email, and phone number of the following staff members: ISO, Network Manager, Systems Manager, Service Desk Manager, Human Resources POC for AUP's	
Network Interconnection Diagram	A copy of the network interconnection diagram that depicts the external: Network Connections, All Firewalls facing other locations / external connections. This may be a PDF, Visio, or PNG.	
Firewall Configuration	Using the guidance requested by your Firewall Administrator, provide a copy of the generated firewall configuration file (with the password hash replaced by 3 Hash Marks ###)	
IP Ranges	Provide a text file that contains the IP ranges of your servers, workstations, and Laptops. You may provide a CIDR notated listing if the space is contagious. Overly broad IP ranges (e.g. /8) will not be accepted. You are expected to know where your IT assets are on the network	
System Hardening Hosts	Provide a text file that identifies the host name and IP address of the following entity nominated hosts for System Hardening Analysis: 3 Workstations; 3 Laptops; 1 Domain Controller; 3 Application Servers	
AD User Listing	Export separate CSV files from your Active Directory containing all: User Accounts; Computer Accounts	
Acceptable Use Policy	Provide a blank copy of the current entity Acceptable Computer Use Policy Acknowledgement form	

Appendix D - Documentation and Policy Listing (CD ROM Delivery)

Policy or Documentation Content Requirement	Name of Entity Provided Document	Page or Paragraph Reference	Provided (Y or N)
Interconnection Policy—Minimum security requirements			
Unauthorized Logon Attempt Policy			
Host / Device Standard Naming Conventions Scheme			
Principal of Lest Privilege Policy; Account Restrictions			
BYOD Device Policy			
System / Device Log Generation and Retention Policy			
System Interconnection Diagram (Network Diagram for Perimeter Connections)			
Continuous Vulnerability Monitoring Program (SAM 5335.1)			
IT Inventory Policy			
Entities NIST System Hardening Standards Policy (Policy and identified baseline settings)			
Entity Configuration Change Control Policy and Documentation of Practice			
Authentication Management and Standards Policy (Password)			
Incident Response Procedures (SOP / Policy)			
Removable Media Usage Policy (Personal Media / Government Furnished Media)			
Network Acceptable Use Policy (AUP)			
FIPS 199 Systems Classification (Overall Systems)			
FIPS 199 Systems Documentation for Assets designed as “High”			
Prior Two All Host Vulnerability Scans Results			
Process for Sharing Security Alerts, Advisories, and Directives with internal stake holders			